Web 2.0 / Social Media Threats and Security (You 2.0)

Brad Weakly
State Information Security Officer
State of Nebraska, Office of the CIO

What is You 2.0?

GeekFill.com

You 2.0 (online and improved)

- It is the difference between you and on-line you.
- It is the difference between work you and personal you
- It is the difference between what you do in everyday life and what you do when on-line
- It is the difference between the risk you would take as an individual and the risks you take with your information
- It is the new you, or at least a new representation of you

You 2.0 and Security

- Shared information is no longer limited:
  - To who you directly know
  - To who is in general proximity to you
  - It is not bound by your view of common sense personal protection.
- The impact of shared information can be greatly exaggerated (for better or worse).
- Information is shared with broad groups with a less manageable form of trust

Data Classification

- You now need to manage 4 identities and determine what to share within each identity (it is important).

- Face to Face personal information
- Face to Face business information
- On-line personal information
- On-line business information

Separation of information

- There are differences between what you should disclose to family, friends, acquaintances, business partners, employers, prospective employers, lawyers, stalkers, thieves, thugs, criminals.

- Have a plan for your on-line presence
- Segregate your information and only place information that is appropriate and where it is appropriate
- Use separate accounts for personal and business activities to enhance the separation

Turning down “friendship”

- Realize what accepting the friend means for your information.
- Let people know that a “personal” account is only for family and the “other” account is for all the other wonderful people you know.
- Remember that online companies do share your information (that the free service does have a price).
- Remember that online information is more public than private

The Forever factor..

- Online information is typically more permanent that you might think.
- Prospective employers routinely refer to search engines and social sites to vet prospective employees – and although all the information may not be “officially” used, it certainly paints a picture of behavior and ethics that is scrutinized and utilized.
- “What stays in Vegas” might stay there, but it might be accessible from anywhere in the world.

What you didn't know you were sharing..

- Meta information in/with photos:
  - GPS coordinates of the location
  - Device information
  - Tags about people and things that give great insight into you and your personal habits and your association to others
- Where you work and play - and when
- Personal details
  - Where you live, your family, your birthdate, where you grew up and schools you went to..

But all the information is innocent right?

- youropenbook.org – Search public facebook updates
- Spokeo.com – Information aggregation and search engine..
- Creepy.py – a geolocation aggregator program
- Tineye.com – reverse photo search
- Peekyou.com – “makes people search worthwhile”
- Maltego – data mining application

What is Web 2.0?

- The term Web 2.0 is commonly associated with web applications that facilitate interactive information sharing, interoperability, user-centered design and collaboration on the World Wide Web – Wikipedia.

- Web 2.0 still uses the tools already in place.
- Predominately based on interactive tools.
- More feature rich than passive web surfing.
- More potential avenues of exploitation.

Is there a difference between Web 2.0 & Social Media Websites?

- Social media websites allow the creation and exchange of user-generated content. Social media uses web-based technologies to turn communications into interactive dialogues.
- Web 2.0 – Collaborative web environment (social media sites, blogs, wikis, mashups).
- Examples:
  - FaceBook
  - MySpace
  - Twitter
  - LinkedIn

Who uses social media sites?

- There are millions of users that log onto social sites everyday!
- Ebizmba.com stats (10/20/2011):
  - Ranked #1, Facebook has 700 Million unique monthly visitors
  - #2, Twitter 200 Million unique monthly visitors
  - #3, LinkedIn 100 Million unique monthly visitors
- Among all online adults, 91% use social media sites every month – Experian Oct. 2011 Social Media Consumer Trend Report

Social Media is evil right?

- Right or wrong, it is here to stay – we must find ways of addressing the issues and start to utilize the new technologies effectively.
- Social media sites are effective tools used to enhance communication. Those tools although generally used for positive impact, can certainly be used for somewhat less than desirable purposes.
- Social sites are public sites and although they certainly work to protect that information, content is regularly disclosed by accident or malicious action.

Security issues related to the use of Social Media sites:

- Spam – Oct 26th International report - spammers utilize more public URL shortening services..
- Spyware
- Worms
- XSS (Cross-site Scripting) vulnerabilities
- Flash Attacks
- Phishing
- Spearphishing
- Mouseovers

Why would anyone want my information?

- Information is money, or can be utilized in a way to make money.
- Attacks on social media sites will increasingly become more financially driven.
- Social media sites are a treasure trove of information that can be used to carry out identity theft (or worse).

"Seven Deadly Sins of Social Networking Security" – CSO Mag.

- 1. Over-sharing organization activities.
- 2. Mixing personal with professional; Commonly on Facebook, where one's friends included business associates, family members and friends.
- 3. Engaging in Tweet (or Facebook/LinkedIn/Myspace) rage. Imagine you are at a party where everyone is listening, including your boss, spouse and future employer.
- 4. Believing he/she who dies with the most connections wins. Always verify the person who wants to get in contact with you.

“Seven Deadly Sins of Social Networking Security” continued..

- 5. Password sloth. Using the same password on several sites is like trusting the weakest link in a chain to carry the same weight.
- 6. Trigger finger (clicking on everything). Inboxes contain everything from drink requests to cause requests, do not get into the click habit unless you are ready to deal with drive-by downloads and zero-day attacks.
- 7. Endangering yourself and others. Too much information on your spouse, children or others can expose them to identity theft or worse.

Current threats/issues:

- Social media site “privacy breaches”.
- Confidential business information leakage.
- Shortened URLs (http://bit.ly/a1b2c3, http://tinyurl.com/somethinginteresting) are unchecked and do not give any clues to the source or its content.
- New avenues of malware and infection.
- Banner ad hijacking.
- Friending someone you do not know.
- Lack of a business policy or lack of enforcement.

How to protect yourself and your organization:

- Top strategic action – become aware of the risks involved with social media sites.
- Social networks do not encourage strong password selection. Choose complex passwords!
- Avoid using the same password on multiple sites and do not synchronize account information with organization login credentials.
- TMI (too much information). Although it is a great idea to let your neighbors know you will be out on vacation so they can keep an eye on your house, it is NOT a great idea to post those vacation plans on a public site.

Protection, continued..

- Avoid leaking sensitive data about the organization. Mentioning something to your best friend is absolutely different than publishing something online so a friend (and potentially the world) can see it and indiscriminately forward it to others in its original form.
- Think twice about including GPS information in your online information, think again before adding home address and personal information. It is all valuable information that enables extremely accurate profiling and attack targeting.

Protection, continued..

- Set your settings to high privacy and/or enable security settings on the sites you use.
- Review a given Website's privacy policy, you may be surprised on what you are actually agreeing to.
- Log off when you leave.
- Install and update antivirus software.
- Keep system software AND applications up to date.
- Make sure the connection you use is secure.

Securing mobile devices

- Know the threats - As any carny knows, the easiest mark is one who is not paying attention.
- The principle threat to phones is the loss or theft of the device (but application exploits are on the rise).
- Use only approved app stores
- Check the bills
- A “jail broken” device is much more easily compromised than one running a current “stock” image
- Android – pay attention to the rights you give apps

Tools:

- Firesheep - http://codebutler.com/firesheep A firefox browser plugin that captures logins and cookies then logs into that users account AS THAT USER! Classic identity theft in action.
- Https Everywhere https://www.eff.org/https-everywhere Many sites on the web offer some limited support for encryption over HTTPS, but make it difficult to use. This plugin rewrites requests to those sites to utilize HTTPS (works with Google Search, Twitter, Facebook, most of Amazon).

More tools:

- SOPHOS Social Media Security toolkit: http://www.sophos.com/lp/threatbeaters/toolkit-contents.html
- Last Pass: http://lastpass.com/ Free password (and pay version) manager for mainstream browsers and multiple operating systems including Windows, Mac and Linux.
- 1Password: https://agilebits.com/onepassword Password manager for systems and mobile devices (not free)

Information Sources:

- Reclaim Privacy: http://www.reclaimprivacy.org/
- Def Con 19: http://www.defcon.org/
- Dark Reading: http://darkreading.com
- SANS: http://sans.org
- Department of Homeland Security: http://www.dhs.gov/stopthinkconnect
- Onguard: http://onguardonline.gov/
- ID Theft: http://www.ftc.gov/bcp/edu/microsites/idtheft/